IN THE CLAIMS

Please cancel claims 2, 6, and 9-12 without prejudice or disclaimer, and amend claims 1 and 5 as follows:

1. (Currently Amended) A tamper-resistant fault detection method for an IC card including an information processing device mounted thereon, comprising the steps of:

(1) performing a DES (data encryption standard) symmetric-key encryption process $Z = E(M, K)$ in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z in a memory in the IC card;

(2) performing a corresponding DES decryption process $W = D(Z, K)$ for said process result Z stored on said memory and storing the decryption result W on the memory;

(3) outputting said processing result Z from said information processing device when said processing result W coincides with said plaintext M; and

(4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M.

2. (Cancelled)

3. (Previously Presented) The encryption processing method of claim 1 wherein said information processing device is reset as a control method of suppressing the output of said processing result.

4. (Previously Presented) The encryption processing method of claim 1 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit to be mounted on an IC card.

5. (Currently Amended) A tamper-resistant fault detection method for an IC card including an information processing device mounted thereon, comprising the steps of:

(1) performing a DES (data encryption standard) symmetric-key decryption process $Z = D(C, K)$ wherein a secret key K is to be applied to an input ciphertext C, and storing the processing result Z on a memory in the IC card;

(2) performing a corresponding DES encryption process $W = E(Z, K)$ for the processing result Z stored on said memory, and storing the result W on the memory;

(3) outputting said processing result Z from said information processing device when said processing result W coincides with said ciphertext C; and

(4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said ciphertext C.

6. (Cancelled)

7. (Previously Presented) The decryption processing method of claim 5 wherein said information processing device is reset as a method of suppressing the output of said processing result.

8. (Previously Presented) The decryption processing method of claim 5 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit.

9-12. (Cancelled)